REMARKS

Applicant respectfully requests consideration and allowance of the pending claims. Claims 1, 8 and 15 are independent. Claims 1-2, 4, 7-9, 11, 14-16 and 18 are amended hereby. Applicant thanks the Examiner for the detailed analysis presented in the Office Action of April 5, 2007.

Double Patenting

Claims 1-20 stand rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-6, 8-18, 20-29, 31-40 and 42-47 associated with U.S. Patent Application No. 10/609,260. The Applicant acknowledges the Double Patenting rejection. However, because claims may be amended during the prosecution of the instant Application and/or Application No. 10/609,260, Applicant requests that the Double Patenting rejection be held and abeyance until such a time that the Office indicates allowable subject matter.

Claim Objections

The Office has objected to **claims 2, 4, 9, 11, 16 and 18**. The Office submits that the claims include a number of informalities. To address the objected to claims, Applicant has added subject matter that clarifies the group notation represented by Z^*_P. Nonetheless, Applicant respectfully submits that those of ordinary skill in the art in technologies related to cryptography understand such group notations. Regarding the notation $x \xleftarrow{R} Z^*_P$, Applicant respectfully submits that adding clarifying subject matter to the objected to claims is unnecessary. In particular, those of ordinary skill in the art and technologies

related to cryptography understand that the notation indicates the random selection of x from the group Z^*_P. Accordingly, Applicant requests reconsideration and withdrawal of the objections to the claims.

Claim Rejections Under 35 U.S.C. § 101

Claims 1, 8 and 15 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Applicant respectfully traverses the rejection.

Claims 1 and 8 have been amended to recite "disseminating the second data to a computing device." Applicant respectfully submits that the subject matter added to the rejected claims overcomes the rejection under 35 U.S.C. § 101. Accordingly, the Office is respectfully requested to withdraw the rejection.

As far as the rejection of **claim 15** is concerned, Applicant believes that the Office has improperly rejected the claim. In particular, the subject matter of rejected independent claim 15 relates to an apparatus. The apparatus includes at least a memory and signature generating logic. The signature generating logic is defined as being "operatively coupled to said memory and configured according to parameter data so as to be capable of encrypting data based on a Jacobian of at least one curve, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve, determine private key data and corresponding public key data, and generate second data by signing said first data with said private key data, said second data having a corresponding blind digital signature, said blind digital signature corresponding to a single element in said Jacobian of said at least one curve." Therefore, contrary to that asserted by the Office, the tangible result (i.e., an apparatus) of the subject matter recited by claim 15 includes both a memory and

signature generating logic associated with an apparatus. Accordingly, the Office is respectfully requested to withdraw the rejection.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-20 stand rejected as being unpatentable under 35 U.S.C. § 103(a) in view of a publication to Boldyreva ("Efficient Threshold Signature, Multisignature Schemes Based On The Gap-Diffie-Hellman-Group Signature Scheme") and Zhang et al. ("ID-Based Blind Signature and The Rating Signature from Pairings") ("Zhang"). Applicant respectfully traverses this rejection.

Applicant addresses the rejection of the independent claims in the following. As a preliminary matter, Applicant does not separately address the patentability of each remaining dependent claim in detail. However, Applicant's decision not to discuss the differences between the cited art and each dependent claim should not be considered as an admission that Applicant concurs with the Office's conclusion that these dependent claims are not patentable over the disclosure in the cited references. Similarly, Applicant's decision not to discuss differences between the prior art and every claim element, or every comment made by the Office, should not be considered as an admission that Applicant concurs with the Office's interpretation and assertions regarding those claims. Indeed, Applicant believes that all of the dependent claims patentably distinguish over the references cited. Moreover, a specific traverse of the rejection of each dependent claim is not required, since dependent claims are patentable for at least the same reasons as the independent claims from which the dependent claims ultimately depend.

Amended Claim 1 recites:

> A method comprising:
> receiving first data to be blindly signed;
> establishing parameter data for use with signature generating logic that *encrypts data based on a Jacobian of at least one curve*, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve;
> determining private key data and corresponding public key data using said signature generating logic;
> generating second data by signing said first data with said private key data using said signature generating logic, said second data having a corresponding blind digital signature, *said blind digital signature corresponding to a single element in said Jacobian of said at least one curve*; and
> disseminating the second data to a computing device. (Emphasis added.)

Respectfully, none of the references, alone or in combination, discloses or suggests what is recited by **claims 1, 8 and 15** for at least the following reasons.

As those of ordinary skill in the art appreciate, current digital signature schemes, such as those based on conventional Computational Diffie-Hellman assumptions, produce relatively long digital signatures in an attempt to improve security. However, such long digital signatures are not generally user friendly. Coupled with the novel use of a Jacobian of at least one curve, a "blind digital signature corresponding to a single element in said Jacobian of said at least one curve" may be generated from the novel limitations recited by claims 1, 8 and 15. Using the Jacobian of at least one curve enables the use of a much simplified blind digital signature (e.g., a blind digital signature that corresponds to a signal element in the Jacobian).

Boldyreva discloses a conventional blind signature scheme based on the use of the conventional Gap Diffie-Hellman (GDH) group. The blind signature scheme is discussed in detail in Section 6, page 12, of the Boldyreva document.

The detailed description of the indicated Section clearly shows that Boldyreva does not disclose or suggests producing a blind digital signature that corresponds to a "single element" in a "Jacobian of at least one curve." Therefore, the Boldyreva publication does not disclose or suggest at least two limitations set forth by independent claim 1.

The Office has relied upon Zhang to show that GDH groups may be derived from a Jacobian of a curve. The Office points to page 7, first paragraph, of the Zhang publication. However, the same section of the relied upon publication also describes that a derived "signature consists of an element in G and an element in V." Therefore, the signature includes at least two elements.

Therefore, even if one of ordinary skill in the art were to combine the teachings of the Zhang with those of Boldyreva, which the Applicant does not concede, the combination does not teach or suggest at least producing a "blind digital signature corresponding to a single element in said Jacobian of said at least one curve." (Claim 1.)

According to the foregoing, Applicant respectfully submits that the combination of Boldyreva in view of Zhang neither discloses nor suggests the limitations of claim 1. Similarly, the combination of Boldyreva in view of Zhang fails to disclose or suggest what is recited in claim 8. In particular, the combination fails to disclose or suggest at least "said blind digital signature corresponding to a single element in said Jacobian of said at least one curve." (Claim 8.) Moreover, the combination of Boldyreva in view of Zhang fails to disclose or suggest what is recited in claim 15. In particular, the combination fails to disclose or suggest at least "said blind digital signature corresponding to a single element in said Jacobian of said at least one curve." (Claim 15.) Claims 2-

7, 9-14 and 16-20 are at least allowable due to their dependency upon an allowable independent claim, as well as for additional limitations set forth by the claims.

The detailed discussion above shows that Boldyreva and Zhang, whether taken alone or in combination together, fail to disclose or suggest the claims rejected under 35 U.S.C. § 103(a). Accordingly, reconsideration and withdrawal of the rejection are respectfully requested.

Conclusion

In accordance with the foregoing remarks, Applicant believes that the pending claims are allowable and the application is in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Should the Examiner have any further issues regarding this application, the Examiner is requested to contact the undersigned attorney for the Applicant at the telephone number provided below.

Respectfully Submitted,

Dated: July 3, 2007

By: / Lewis C Lee Reg No 34656 /
Lewis C. Lee
Reg. No. 34,656
(509) 324-9256